Amendments to the Claims

Please amend Claims 1, 31 and 55. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. (Currently Amended) An apparatus for regulating data flow to a network comprising:

a mechanical lock assembly having multiple activated positions that is activated by turning a key; and

an electronic circuit that senses a position of the key in the lock assembly to ~~enable~~ regulate a flow of data information to a target network based on data flow rules selected by the position of the key.

2. (Original) An apparatus as in claim 1, wherein the data information is intercepted and decoded by the electronic circuit to identify requests for data available on the network, and the data information including a request for data is transmitted to a target network when the key is in an enabling position of the lock assembly.

3. (Original) An apparatus as in claim 1, wherein the data information includes network data packets transmitted to a wide area network from which information is accessed.

4. (Original) An apparatus as in claim 1, wherein the network is the Internet.

5. (Original) An apparatus as in claim 1, wherein the electronic circuit has access to a database of data flow rules for determining which data information is allowed to flow to the network.

6. (Original) An apparatus as in claim 5, wherein the electronic circuit decodes the data information to determine a URL (Uniform Resource Locator) indicating a target address on the network from which information is to be accessed, the electronic circuit enabling

further transmission of the data information to the target address based on data flow rules and a position of the key in the lock assembly.

7. (Original) An apparatus as in claim 5, wherein the electronic circuit decodes the data information to determine an IP (Internet Protocol) target address indicating to which network address a data packet is directed, the electronic circuit enabling further transmission of the data information to the target address based on data flow rules and a position of the key in the lock assembly.

8. (Original) An apparatus as in claim 1, wherein the data information is generated by a user at a computer on a first network and the data information is transmitted to a target address on a second network.

9. (Original) An apparatus as in claim 8, wherein the target address on the second network is a server.

10. (Original) An apparatus as in claim 1, wherein the data information includes a request for web page information.

11. (Original) An apparatus as in claim 1, wherein the electronic circuit enables a flow of data information to a target network based upon a provided password.

12. (Original) An apparatus as in claim 11, wherein the password is provided by a user attempting to access information from a target address.

13. (Original) An apparatus as in claim 11, wherein the password is provided by a person activating the lock assembly by turning the key.

14. (Original) A device for regulating data information transmitted through a communication link, the device comprising:

a sensing unit that detects a position of a switch coupled to a lock assembly, the switch being activated by turning a key to a position in the lock assembly;

a memory device for storing data flow rules of the communication link; and

a communication controller that intercepts the data information transmitted through the communication link and, based on the data flow rules as selected by a position of the switch and a provided password, regulates a further flow of the data information through the communication link.

15. (Original) A device as in claim 14, wherein the data information is transmitted through the communication link as data packets and the communication controller regulates a flow of the data packets to target destinations based on a content of the data packets.

16. (Original) A device as in claim 14, wherein the data information is decoded to determine whether the corresponding intercepted data information shall be transmitted to a target destination through the communication link.

17. (Original) A device as in claim 14, wherein the communication controller regulates a flow of data information based on which of multiple possible sources generates the data information, allowing certain sources to transmit data information to a target address through the communication link.

18. (Original) A device as in claim 14, wherein the data flow rules include information indicating circumstances in which intercepted data information shall be blocked from further transmission through the communication link to a target destination.

19. (Original) A device as in claim 14, wherein the communication controller decodes the data information to determine a URL (Uniform Resource Locator) indicating a target address from which information is to be accessed, the communication controller enabling further transmission of the data information to the target address based on the data flow rules as selected by a position of the key in the lock assembly and the provided password.

20. (Original) An apparatus as in claim 14, wherein the communication controller decodes the data information to determine an IP (Internet Protocol) destination address indicating to which of multiple possible network addresses the data information is directed, the communication controller enabling further transmission of the data information to the destination address based on the data flow rules as selected by a position of the key in the lock assembly and provided password.

21. (Original) An apparatus as in claim 14, wherein the communication link supports data information flows of multiple session types and the data flow rules indicate which session types shall be supported by the communication link, the communication controller further transmitting intercepted data information associated with allowed session types based on a position of the key in the lock assembly in conjunction with the provided password.

22. (Original) An apparatus as in claim 14, wherein the restriction criteria indicates at what time of day information can be accessed from a target address.

23. (Original) A device as in claim 22, wherein the restriction criteria includes information indicating from which addresses intercepted data information shall be blocked from further transmission through the communication link to a target destination.

24. (Original) An apparatus as in claim 14, wherein the data information is generated by a user at a computer on a first network and the data information is transmitted through the communication link to a target address on a second network.

25. (Original) An apparatus as in claim 24, wherein the target address on the second network is a server.

26. (Original) An apparatus as in claim 14, wherein the data information includes a request for web page information.

27. (Original) An apparatus as in claim 14, wherein the data information is an e-mail message.

28. (Original) An apparatus as in claim 27, wherein the e-mail message is transmitted to a target address depending on the author of the message and to which address the e-mail message is directed.

29. (Original) An apparatus as in claim 14, wherein the password is provided by a user attempting to transmit corresponding data information through the communication link.

30. (Original) An apparatus as in claim 14, wherein the password is provided by a person activating the switch by turning a key in the lock assembly.

31. (Currently Amended) A method of limiting access to a network, the method comprising:

sensing a position of a switch having multiple activated positions coupled to a lock assembly activated by turning a key; and

~~enabling~~ regulating a flow of data information to the network through a communication link based on data flow rules selected by the ~~a~~ position of the switch.

32. (Original) A method as in claim 31, wherein the step of enabling a flow of data information includes:

intercepting the data information;

decoding the data information to identify requests for information available on the network; and

based on a position of the switch, transmitting the data information including requests to a corresponding target address or blocking the data information from a target address.

33. (Original) A method as in claim 31, wherein the data information includes network data packets transmitted to a wide area network from which information is accessed.

34. (Original) A method as in claim 31, wherein the network is the Internet.

35. (Original) A method as in claim 31 further comprising the step of:

accessing a database of data flow rules for determining which data information is allowed to flow to the network.

36. (Original) A method as in claim 35 further comprising the steps of:

decoding the data information to determine a URL (Uniform Resource Locator) indicating a target address on the network from which information is to be accessed; and

enabling further transmission of the data information to the target address based on data flow rules and a position of the key in the lock assembly.

37. (Original) A method as in claim 35 further comprising the steps of:

decoding the data information to determine an IP (Internet Protocol) target address indicating to which network address a data packet is directed; and

enabling further transmission of the data information to the target address based on data flow rules as selected by a position of the key in the lock assembly.

38. (Original) A method as in claim 31, wherein the data information is generated by a user at a computer on a first network and the data information is transmitted to a target address on a second network.

39. (Original) A method as in claim 38, wherein the target address on the second network is a server.

40. (Original) A method as in claim 31, wherein the data information includes a request for web page information.

41. (Original) A method as in claim 31, further comprising the step of:

enabling a flow of data information to a target network based upon a provided password.

42. (Original) A method as in claim 41, wherein the password is provided by a user attempting to transmit corresponding data information.

43. (Original) A method as in claim 41, wherein the password is provided by a person activating the lock assembly by turning the key.

44. (Original) A method for regulating data information transmitted through a communication link, the method comprising:

intercepting data transmitted through the communication link;

determining a position of a key in a lock assembly;

accessing data flow rules stored in a memory device; and

transmitting the intercepted data information to a target address based on data flow rules in the memory device as selected by a position of the key in the lock assembly and a provided password.

45. (Original) A method as in claim 44, wherein the data information includes network data packets transmitted to a wide area network from which information is accessed.

46. (Original) A method as in claim 44, wherein the network is the Internet.

47. (Original) A method as in claim 44 further comprising the steps of:

decoding the data information to determine a URL (Uniform Resource Locator) indicating a target address on the network from which information is to be accessed.

48. (Original) A method as in claim 44 further comprising the steps of:

decoding the data information to determine an IP (Internet Protocol) target address indicating to which network address a data packet is directed.

49. (Original) A method as in claim 44, wherein the data information is generated by a user at a computer on a first network and the data information is transmitted to a target address on a second network.

50. (Original) A method as in claim 49, wherein the target address on the second network is a server.

51. (Original) A method as in claim 44, wherein the data information includes a request for web page information.

52. (Original) A method as in claim 44 further comprising the step of:

enabling a flow of data information to a target network based upon a provided password.

53. (Original) A method as in claim 52, wherein the password is provided by a user attempting to transmit corresponding data information.

54. (Original) A method as in claim 52, wherein the password is provided by a person activating the lock assembly by turning the key.

55. (Currently Amended) A method of limiting access to a network, the method comprising:

means for sensing a position of a switch having multiple activated positions coupled to a lock assembly activated by turning a key; and

means for ~~enabling~~ regulating a flow of data information to the network through a communication link based on ~~a~~ data flow rules selected by the position of the switch.